# (12) UK Patent Application (19) GB (11) 2 254 225 (13) A

(43) Date of A publication 30.09.1992

(21) Application No 9203592.2

(22) Date of filing 20.02.1992

(30) Priority data
(31) 664774 (32) 05.03.1991 (33) US

(71) Applicant
National Semiconductor Corporation

(Incorporated in the USA - Delaware)

2900 Semiconductor Drive, PO Box 58090,
Santa Clara, California 95051-8090,
United States of America

(72) Inventors
Wai Tak Chiu
Kwong Yin Wong

(74) Agent and/or Address for Service
Bowles Horton
Felden House, Dower Mews, High Street,
Berkhamsted, Herts, HP4 2BL, United Kingdom

(51) INT CL$^5$
H04M 1/66

(52) UK CL (Edition K)
H4L LECTS L1H3

(56) Documents cited
GB 2217151 A GB 2154395 A EP 0196834 A2
WO 85/02738 A1

(58) Field of search
UK CL (Edition K) H4L LECTS
INT CL$^5$ H04M 1/66 1/72

## (54) Cordless telephone security coding

(57) The security of a cordless telephone system is increased by automatically altering the security code information stored in the cordless telephone handset and base unit. The updating of the security code is performed at any convenient time or in response to any convenient activity, such as the placement of the handset into the base unit for storage and recharging. In one embodiment when the security code is to be updated a new security code is generated, for example by random number generation, by the handset. This information, together with information indicating that the security code is to be updated, is sent from the handset to the base unit, via the RF link normally used for wireless communication between the handset and the base unit or via a direct link established when the handset is placed in a receiving cradle on the base unit.

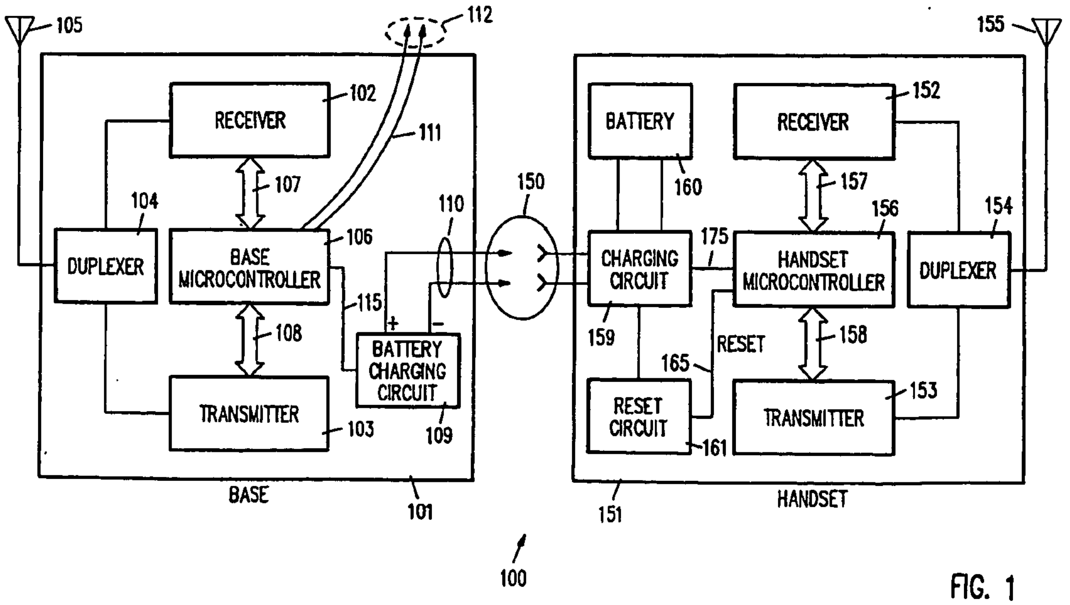

FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed copy.

GB 2 254 225 A

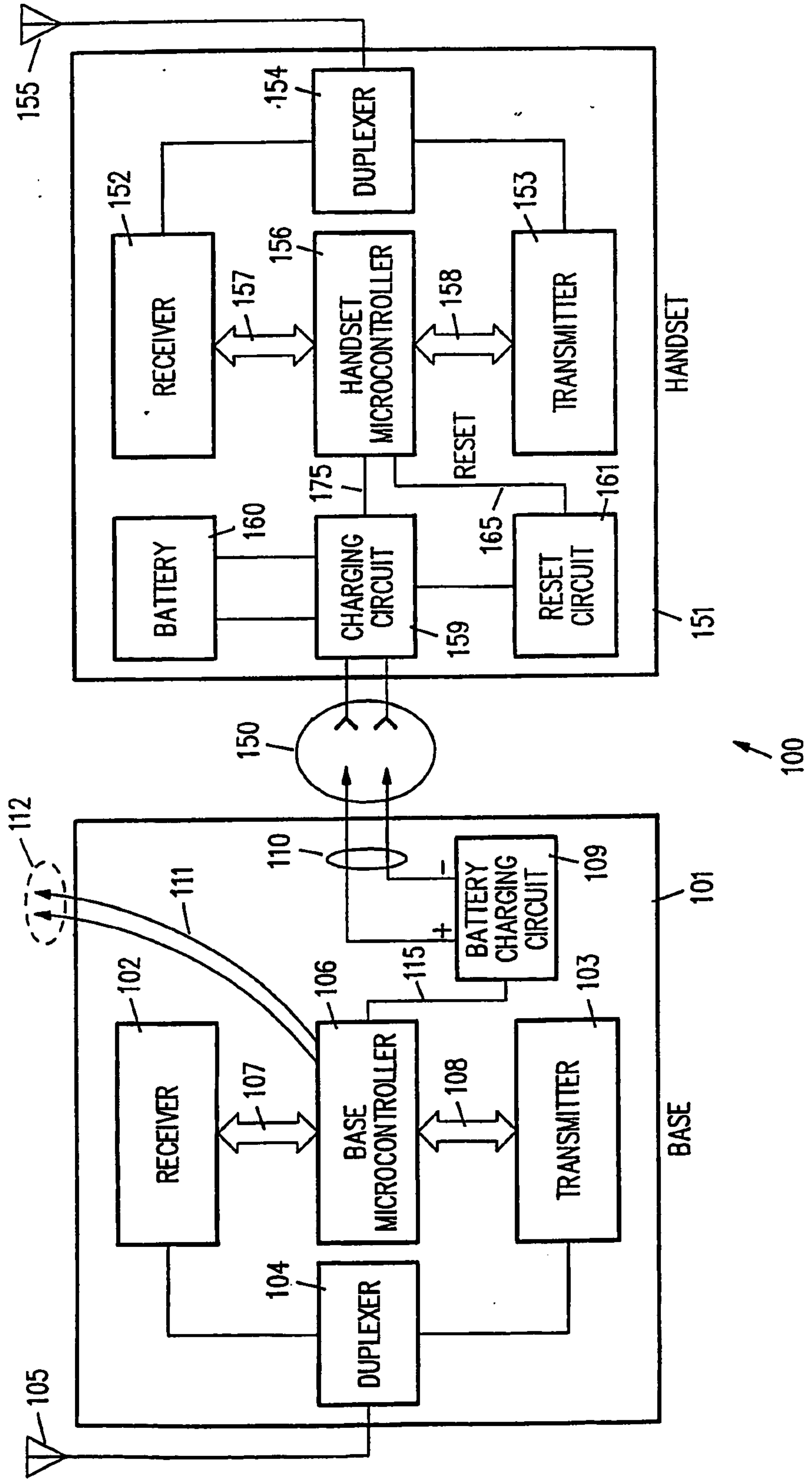
155
DUPLEXER
154
152
RECEIVER
157
156
HANDSET MICROCONTROLLER
158
153
TRANSMITTER
HANDSET
RESET
175
165
161
BATTERY
160
CHARGING CIRCUIT
159
RESET CIRCUIT
151
150
100
112
111
110
+
−
BATTERY CHARGING CIRCUIT
109
101
115
102
106
103
RECEIVER
107
BASE MICROCONTROLLER
108
TRANSMITTER
BASE
104
DUPLEXER
105

FIG. 1

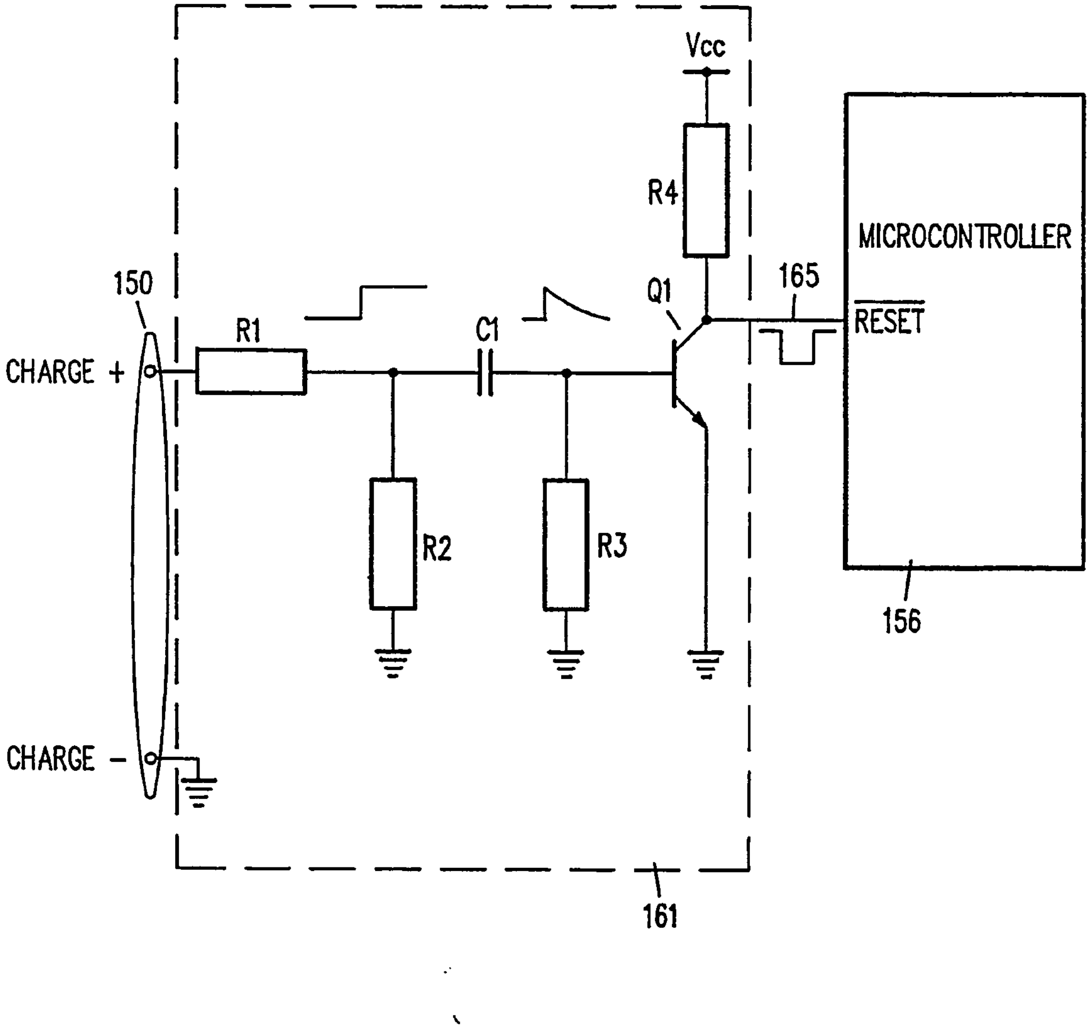
Vcc
R4
MICROCONTROLLER
165
150
Q1
RESET
R1
C1
CHARGE +
R2
R3
156
CHARGE −
161

FIG. 2

HANDSET FLOW CHART

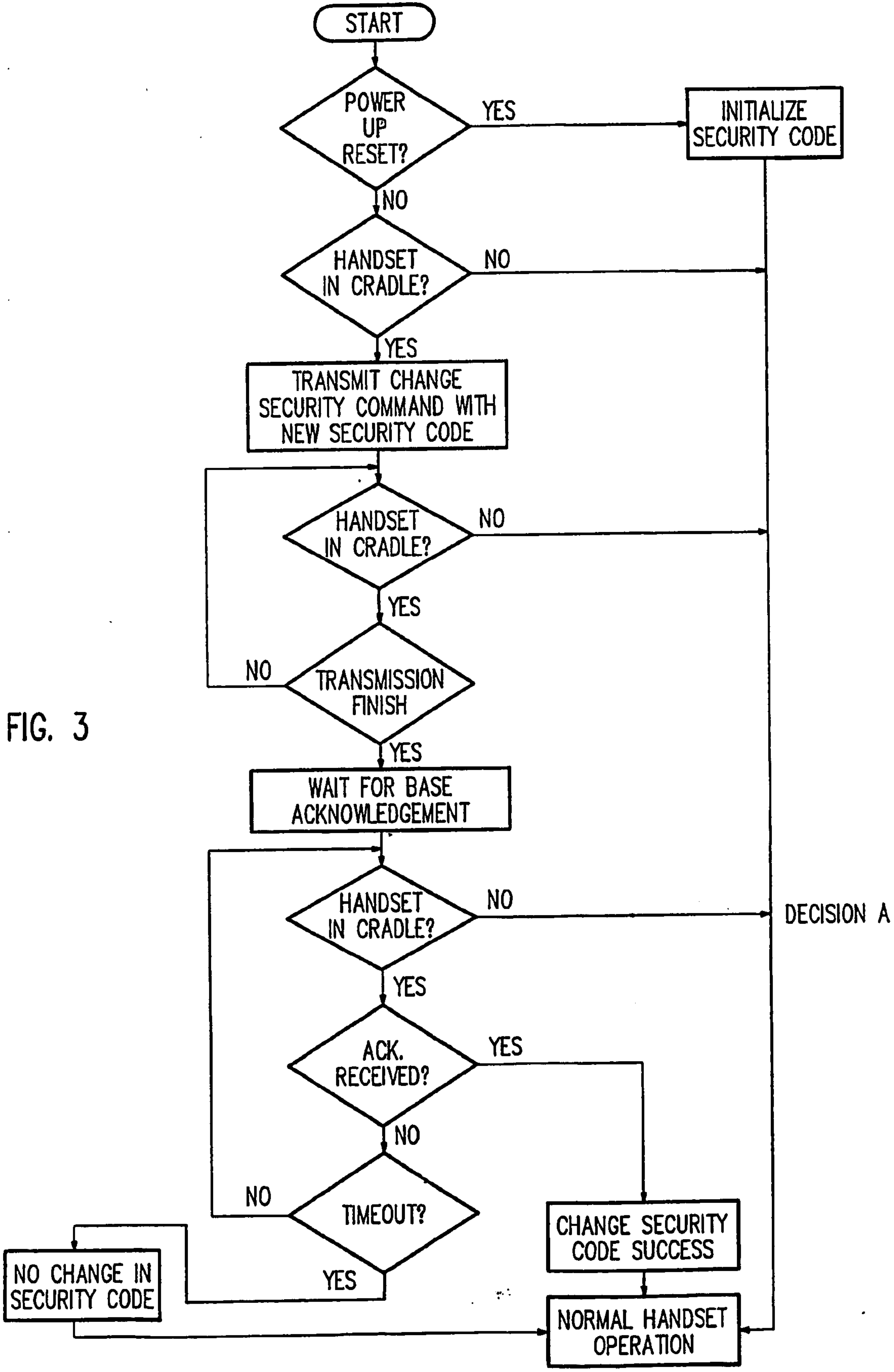

FIG. 3

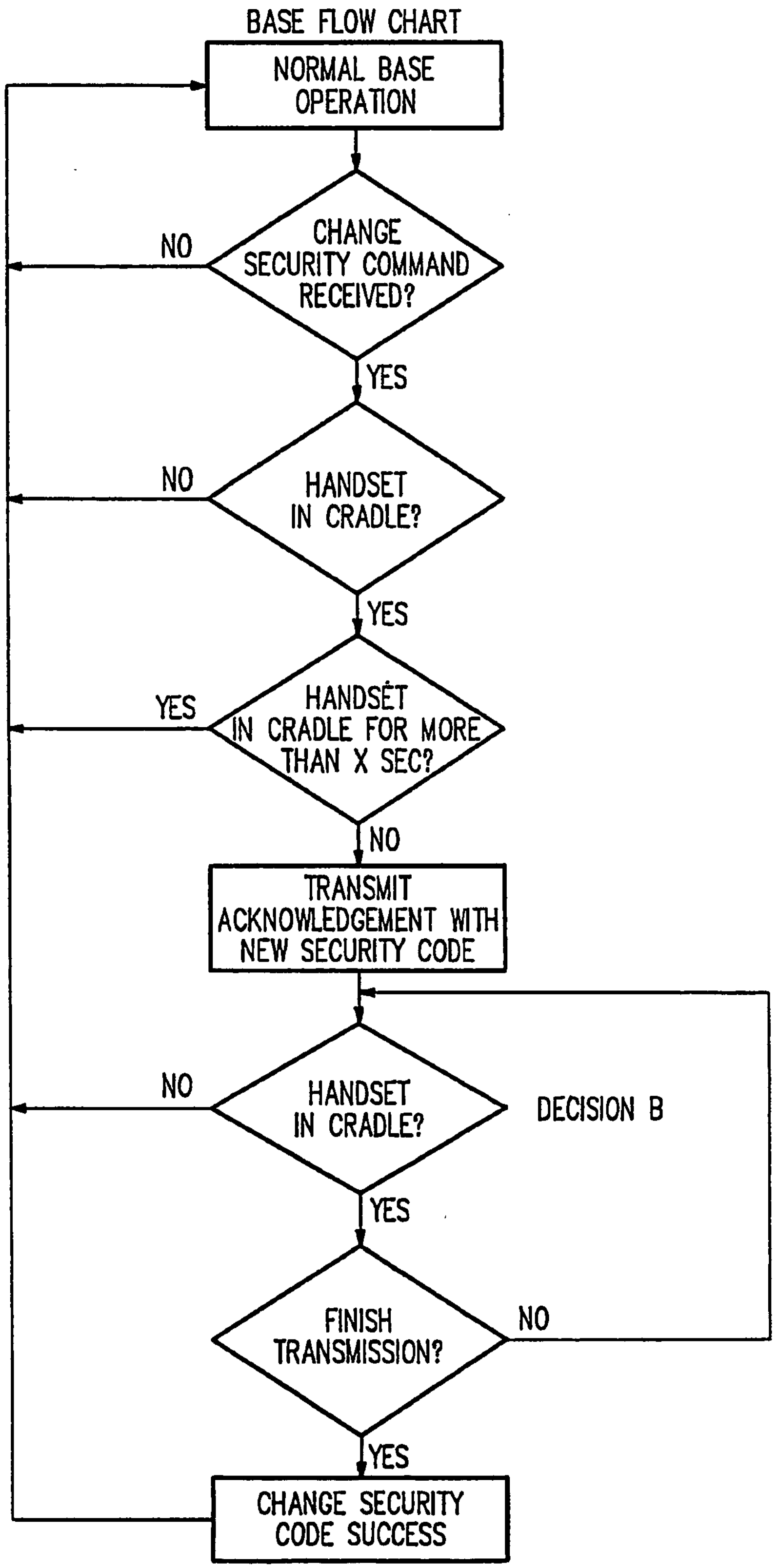
BASE FLOW CHART
NORMAL BASE OPERATION
CHANGE SECURITY COMMAND RECEIVED?
NO
YES
HANDSET IN CRADLE?
NO
YES
HANDSÉT IN CRADLE FOR MORE THAN X SEC?
YES
NO
TRANSMIT ACKNOWLEDGEMENT WITH NEW SECURITY CODE
HANDSET IN CRADLE?
DECISION B
NO
YES
FINISH TRANSMISSION?
NO
YES
CHANGE SECURITY CODE SUCCESS

FIG. 4

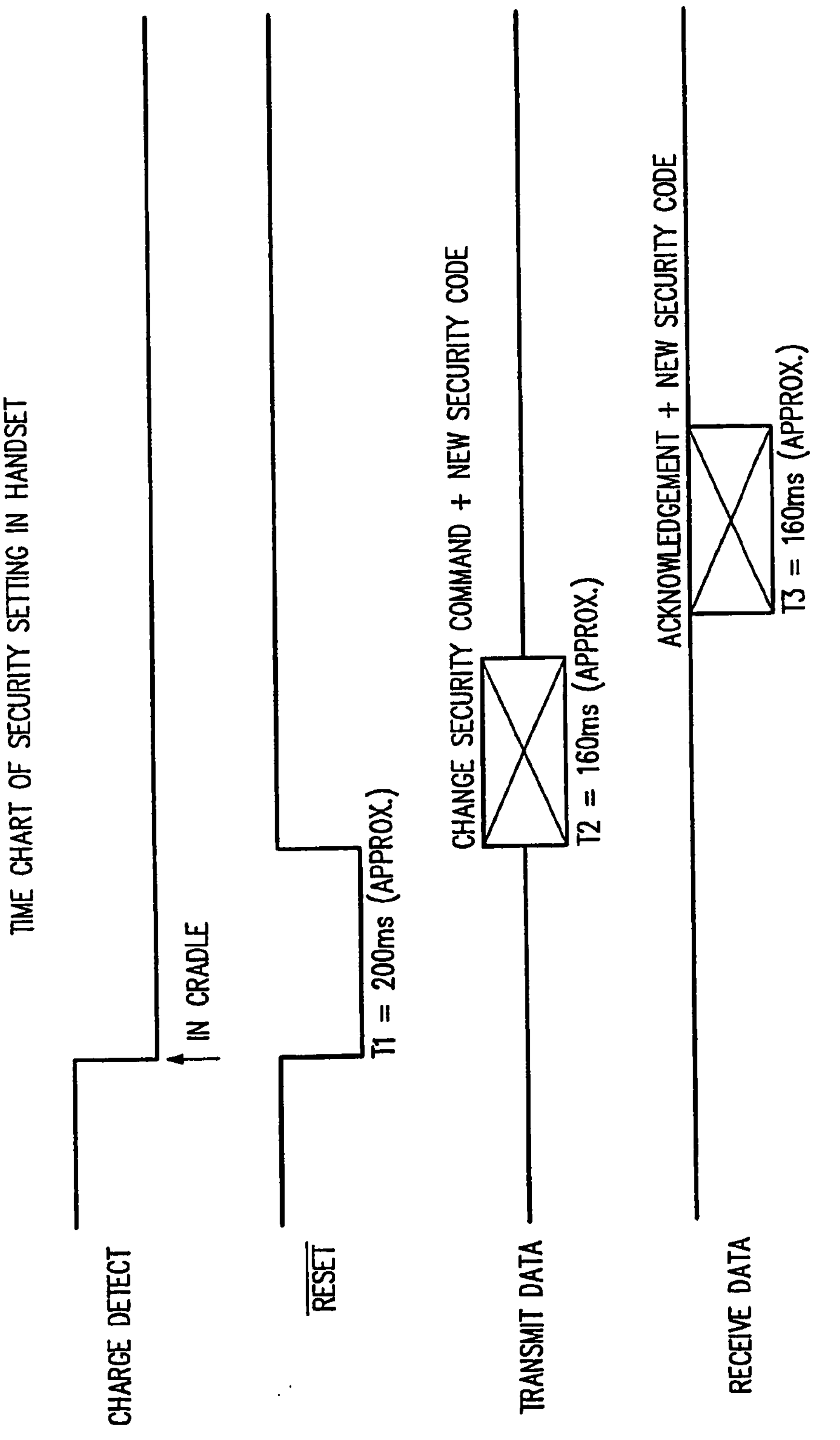
TIME CHART OF SECURITY SETTING IN HANDSET
CHARGE DETECT
IN CRADLE
RESET
T1 = 200ms (APPROX.)
TRANSMIT DATA
CHANGE SECURITY COMMAND + NEW SECURITY CODE
T2 = 160ms (APPROX.)
RECEIVE DATA
ACKNOWLEDGEMENT + NEW SECURITY CODE
T3 = 160ms (APPROX.)

FIG. 5

# CORDLESS TELEPHONE SECURITY CODE

## INTRODUCTION

This invention pertains to communications, and particularly to portable communication systems such as a hand held telephone which includes a base unit and a handset.

## Background of the Invention

Since their introduction, hand held or "cordless" telephones have enjoyed a substantial popularity. Such telephones include a hand held unit or "handset" which looks much like a telephone but includes means for establishing a duplex radio link over a channel having two frequencies with a base unit which is hard wired to the telephone line. In use, communication is established between the base unit and the handset either upon initiation of a call by the handset user, or an incoming telephone call received over the telephone line. To the user, the handset must function as much as a standard telephone as possible, while providing mobility. The handset typically includes rechargeable batteries such as nicads which are recharged by placing the handset in the base unit for convenient storage and electrical connection to a battery charging power supply.

Given the fixed amount of radio spectrum, only a relatively small portion has been allocated to cordless telephones. Since cordless telephones are to a large degree unregulated and, unlike mobile phones or cellular telephones significantly less sophisticated, they inherently have certain limitations. Cordless telephones operate on a selected band of a relatively few channels. The selection is made somewhat permanently, i.e., by hardwiring or by the setting of a switch which may or may not be readily accessible by the user. Typically, the base unit and the handset are set to the same channel once and the channel setting is not changed thereafter. In fact, it is likely that few end users are actually aware of the ability to change channels in those cordless telephones which have this capability.

Regardless of whether a given cordless telephone has the ability to select one of a plurality of channels for use, the likelihood is high that a particular location may be undesirably within the communication range of more than one cordless telephone user on the same channel. Given the relative density of urban and suburban areas, and the desirability of having a cordless phone with sufficient communication range to allow its use within a reasonable proximity of a dwelling, a number of cordless telephone users in a given neighborhood may find themselves causing radio frequency interference with their neighbor's cordless telephones. Given also the relatively small number of channels used for cordless telephones, it is also relatively simple for a person to select a channel on his cordless telephone which is the same as the channel of another user. While this may allow an interloper to eave drop on another's conversation, perhaps more dangerous is the potential for the interloper to gain access to a neighbor's telephone line, allowing the interloper to answer or place calls on the neighbor's telephone line.

For these reasons, it is common to employ a security code in cordless telephone systems. Thus, in addition to selecting one of a relatively small number of channels, a cordless telephone user is able to establish a security code, much like a security code is established by persons utilizing remote control garage door openers on a common frequency. A simple security code in the prior art is the sub-audible tone which is encoded by a transmitter and detected by a receiver. If the appropriate one of the standard sub-audible tones is detected, communication is established. If not, communication is not established. A sub-audible tone is lower in frequency than tones which can be heard by the user, so there is no annoying sound heard by the user when the sub-audible tone is used.

A more sophisticated security system utilizes an N bit digital word which is typically transmitted at the beginning of the use of the cordless phone. Utilizing an N bit security code, $2^N$ possible security codes are provided. The security code can either be factory preset so that the cordless handset and base unit include identical security codes, or may be set by the user, for example via DIP switches located on the handset and the base unit. This technique guards, at least to a certain extant, against the possibility of unintentional or unauthorized access to a user's telephone line.

U.S. Patent 4,593,155 describes a cordless telephone system in which the handset is capable of learning the preset security code stored in its associated base unit. U.S. Patent 4,731,813 describes such a cordless telephone system in which communication between the base unit and the handset of the security code information is accomplished by modulating the charging current supplied to the handset from the base unit.

A disadvantage of prior art security systems are that there are a relatively small number of sub-audible tones which can be sequentially tested by a would be intruder. Similarly, while there may be a greater number of digital security codes available, depending upon the number of bits N in the security word, given enough time and patience, a would-be intruder can determine the security code of a neighbor's cordless telephone system merely by trial and error.

Accordingly, there remains the need for providing greater security against would be intruders in cordless telephone systems.

## SUMMARY OF THE INVENTION

According to the teachings of this invention, a novel method and structure are provided for increasing the security of a cordless telephone system. Means are provided for automatically altering the security code information stored in the cordless telephone handset and base unit. Thus, without requiring effort on the part of the user, the security codes are updated to differ from the previous security code setting, while always maintaining corresponding security codes in the handset and base unit.

In accordance with one embodiment of this invention, the updating of the security code is performed at any convenient time interval, or in response to any convenient activity. In one embodiment, such activity is the placement of the handset into the base unit for storage and recharging. Since this activity occurs quite frequently, the security code is updated quite frequently, significantly enhancing security provided to cordless telephones systems constructed in accordance with the teachings of this invention. By updating the security code when the handset is returned to the base unit, the security code is updated roughly in proportion to the amount of usage of the cordless telephone since, as usage increases, battery consumption increases, as is the number of times the handset is returned to the base unit for recharging.

In one embodiment of this invention, when the security code is to be updated a new security code is generated in a predetermined manner, for example by random number generation, by the handset. This information, together with information indicating that the security code is to be updated, is sent from the handset to the base unit, for example to the RF link normally used for wireless communication between the handset and the base unit.

## BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a block diagram depicting a cordless telephone system constructed in accordance with the teachings of this invention;

Figure 2 is a diagram depicting an embodiment of a reset circuit of Figure 1;

Figure 3 is a flow chart depicting the operation of a cordless telephone handset constructed in accordance with the teachings of this invention;

Figure 4 is a flow chart depicting the operation of one embodiment of a cordless telephone and base unit constructed in accordance with the teachings of this invention; and

Figure 5 is a timing diagram depicting the operation of one embodiment of this invention.

## DETAILED DESCRIPTION

Figure 1 is a block diagram depicting one embodiment of a cordless telephone system 100 constructed in accordance with the teachings of this invention. Cordless telephone system 100 includes base unit 101 and handset 151. A base unit 101 and handset 151 communicate control signals, security codes, and telephonic information via radio frequency (RF) utilizing antennas 105 and 155. The only electrical connection between base unit 101 and handset 151 is, if desired, a power connection made via connector 150, to allow base unit 101 to provide battery charging current to handset 151 when handset 151 is physically placed in a cradle within base unit 101.

Base unit 101 includes receiver 102 and transmitter 103, which are coupled on their RF side through duplexer 104 to antenna 105. This allows receiver 102 and transmitter 103 to operate on different frequencies utilizing a common antenna 105. Receiver 102 and transmitter 103 are controlled by base unit microcontroller 106 via busses 107 and 108, respectively. Base unit microcontroller 106 serves to monitor the telephone line which is connected to connector 112 and, via lead 111 to base microcontroller 106. When an incoming call is detected, base microcontroller 106 initiates communication with handset 151 by providing control signals and security codes to transmitter 103. Similarly, base microcontroller 106 receives signals from receiver 102 which were transmitted by handset 151. By providing signals to transmitter 103 and receiving signals from receiver 102, base microcontroller 106 controls the operation of base unit 101 for incoming calls, and calls generated by handset 151.

Base unit 101 also includes battery charging circuit 109. Battery charging circuit 109 serves to provide the appropriate amount of voltage and current to handset 151 for recharging battery 160 when handset 151 is placed in base unit 101. Battery charging circuit 109 typically receives its power from either an AC source (not shown), or from a DC power supply (not shown) used to supply power to base unit 101, for example from an AC source. Battery charging circuit 109 provides battery charging current via leads 110 to connector 150. In accordance with the teachings of this invention, battery charging circuit 109 also includes lead 115 connected to base microcontroller 106. Lead 115 serves to provide a signal to base microcontroller 106 indicating that the handset is in the base cradle for charging.

Handset 151 includes receiver 152 tuned to the frequency of transmitter 103 of base unit 101. Handset 151 also includes transmitter 153 tuned to the frequency of receiver 102 of base unit 101. The RF side of receiver 152 and transmitter 153 are coupled through duplexer 154 to common antenna 155. Handset 151 includes handset microcontroller 156 which communicates control signals with receiver 152 via bus 157, and control signals with transmitter 153 via bus 158. Handset 151 also includes battery 160, such as a nicad battery, since handset 151 is intended for portable operation. Charging circuit 159 serves to charge battery 160 when handset 151 is placed in base unit 101 and thus charging circuit 159 is connected to battery charging circuit 109 via connector 150. In accordance with the teachings of this invention, reset circuit 161 is utilized in order to detect when handset 151 is placed in base unit 101. Circuit 161 provides a reset signal via reset lead 165 to headset microcontroller 156 when battery charging connection is made via connector 150.

Although not shown, handset 151 typically includes a microphone, speaker, and a keypad handset. Handset microcontroller 156 serves to evaluate signals received by receiver 152 and provide signals via transmitter 153 so that base unit 101 and handset 151 communicate with each other only when appropriate control signals are sent and the security code provided by base unit 101 matches the security code provided by handset 151.

Figure 2 is a schematic diagram depicting one embodiment of reset circuit 161 providing a reset signal via lead 165 to handset microcontroller 156. As shown in Figure 2, reset circuit 161 includes resistor R1 connected to the handset side of battery charging connector 150. When handset 151 is placed in base unit 101 such that battery charging circuit 109 of base unit 101 is connected via connector 150 to handset 151, current will flow through resistors R1 and R2. This develops a voltage to turn on transistor Q1 as capacitor C1 charges. This causes a reset pulse to be generated on lead 165, which serves to reset the handset microcontroller, for example in the case of a "deadlock" of the handset microcontroller. This might occur, for example, when the handset battery is first charged as the supply voltage increases gradually and thus may not be able to generate a reset pulse to the handset microcontroller at powerup. The reset circuit shown on Figure 2 also serves to filter a void reset signal bouncing which might otherwise occur when the handset is placed in the cradle of the base unit. When handset 151 is removed from base unit 101, capacitor C1 is discharged through resistors R2 and R3, allowing a reset signal to be generated when handset 151 is once again placed in base unit 101. Typical values for the components of reset circuit 161 of Figure 2 are shown in the following table, and result in a reset pulse having a width of approximately 200 msec.

TABLE 1

| COMPONENT | VALUE |
|---|---|
| R1 | 47k |
| R2 | 390k |
| R3 | 390k |
| R4 | 100k |
| C1 | 1$\mu$F |

Figure 3 is a flow chart depicting the operation of one embodiment of a handset constructed in accordance with the teachings of this invention. When handset microcontroller 156 completes a reset operation, the operation of the flow chart of Figure 3 is started. The handset microcontroller 156 first determines if the reset just completed was a power up reset which is performed, for example, when the battery is charged for the first time. If a powerup reset has just been performed, an initialize security code step is performed in order to set the same default value for the security code so that both handset and base unit have identical security codes and power up.

If the power up reset has not just been performed, the reset must have been a reset caused by placing handset 151 in base unit 101 and thereby causing reset circuit 151 to generate a reset signal on lead 165. In this event, it is determined whether the handset is still in the cradle of base unit 101. This is determined by, for example by the signal provided to handset microcontroller 156 from charging circuit 159 via lead 175, indicating that the handset is being recharged. If the handset is not still in the cradle, normal handset operation continues. However, if handset 151 remains in the cradle, handset 151 provides to base unit 101 a command indicating that the security code should be changed, and a new security code word. This information is transmitted in any convenient fashion, preferably the RF link available between antennas 155 and 105. It is then determined whether handset 151 remains in the cradle. If not, the handset has been removed from the cradle before a security code update was completed. In this event, normal handset operation continues, and the security codeword is not updated. Conversely, if the handset remains in the cradle, it is determined whether the transmission of the command to update the security code has been completed. If not, a check is periodically made to determined whether the handset remains in the cradle. Once the transmission has finished, handset 151 waits for acknowledgement from base unit 101 of the command and the updated security code transmitted to base unit 101. Once this acknowledgement from base unit 101 is received, it is again determined whether handset 151 remains in the cradle of base unit 101. If not, it cannot be known with certainty whether the code update has been performed, and thus normal handset operation is continued and the security codeword is not updated. On the other hand, if handset 151 remains in the cradle, a determination is made as to whether the signal from the base indicates an acknowledgement that the security code has been updated. If yes, handset 151 changes its security code so that the security code stored by base 101 and handset 151 are both updated to the new security code previously selected by handset 151. Normal handset operation then continues with the updated security code.

Conversely, if handset 151 did not receive acknowledgement from base unit 101, a determination is made as to whether a predefined timeout period has expired. If timeout has occurred, there is no change in the security code in handset 151, and normal handset operation continues with the previous security code word. Conversely, if time out has not expired, the decision loop of determining whether the handset remains in the cradle, acknowledgment is received from the base unit, and time out has occurred, is repeated until an exit from this loop is made in one of the three manners just described.

The time delay between the moment handset 151 is placed in the cradle of base unit 101 and handset 151 transmits to base unit 101 a command indicating a security code should be updated is dependent on the width of the reset pulse generated by reset circuit 161, and any desired time delay provided by handset microcontroller 156, for example via well known programming techniques. In one embodiment of this invention, this time delay is approximately 600 msec seconds from the placement of handset 151 into the cradle of base unit 101.

In one embodiment of this invention, during the time in which handset 151 is awaiting acknowledgement from base unit 101, it is not necessary for handset 151 to remain in cradle of base unit 101 so long as good data transmission between the handset and the base unit is achieved so that the up-dating of the security code in both the handset and the base unit may be achieved. In this embodiment, decision step A is not utilized.

Figure 4 is a flow chart depicting the operation of one embodiment of a base unit 101 constructed in accordance with the teachings of this invention, particularly when utilized with a handset 151 which operates in accordance with in the flow chart of Figure 3. As shown in Figure 4, normal base unit operation takes place until base unit 101 receives from handset 151 a command indicating that the security code word should be updated. Upon receipt of the command to update the security codeword, base unit 101 determines if handset 151 remains in the cradle, for example by a signal on the charge detect pin 175. If the handset is no longer in the cradle at this point of the flow chart, normal base operation continues utilizing the old security code word. Conversely, if the handset remains in the cradle, base unit 101 then determines if handset 151 remains in the cradle for more than a predetermined amount of time, for example X seconds typically on the order of one second or less. This is determined, for example, by

X = T1 + N(T2 + T3) + T4; where

T1 = the reset pulse width;
T2 = to transmit a complete 'Change Security Code';
T3 = time required to receive a complete 'Acknowledgement';
T4 = tolerance; and
N = the number of trials to change security (N = 1 in figures 3 and 4)

If no, base unit 101 transmits to handset 151 an acknowledgment with the new security codeword which it has received from handset 151. Base unit 101 then determines whether handset 151 remains in the cradle for a sufficient period of time for base unit 101 to complete its transmission to handset 151. If not, normal base unit operation, utilizing the previous security codeword, resumes. If yes, base unit 101

WHAT IS CLAIMED IS:

1. A cordless telephone comprising:

a base unit including means for storing a base unit security code;

a handset including means for storing a handset security code;

means for authorizing communication between said base unit and said handset when said base unit security code and said handset security code are set to corresponding values;

means for determining that an update to said security codes is desired; and

means for communicating between said handset and said base unit that said security codes are to be updated.

2. A cordless telephone system as in claim 1 wherein said means for communicating comprises an RF link between said handset and said base unit, said RF link also being used for normal cordless telephonic communication between said handset and said base unit.

3. A cordless telephone system as in claim 1 wherein said base unit further comprises a cradle for holding said handset, and said means for communicating comprises a direct link established between said handset and said base unit when said handset is placed in said cradle.

4. A cordless telephone system as in claim 1 wherein said means for determining comprises means responsive to a stimulus selected from the group consisting of: elapsed time, cordless telephone usage, placement of said handset in said cradle; removal of said handset from said cradle, turning on said handset, turning off said handset, and selection of one or more functions on said handset.

5. A cordless telephone system as in claim 1 wherein said means for communicating comprises:

first means within a first of said handset and said base unit for transmitting to the other of said handset and said base unit a command indicating said security codes are to be updated, and a new value associated with said security codes;

second means within said other of said handset and said base unit for updating said security code of said other of said handset and said base unit, and for communicating to said first of said handset and said base unit that said security code of said other has been updated; and

third means within said first of said handset and said base unit to update said security code of said first upon receipt of said communication from said other.

6. A cordless telephone system as in claim 5 wherein said first means operates in response to the charging of said handset when said handset is placed in said cradle.

7. A cordless telephone system as in claim 3 wherein said direct link is established utilizing the charging current supplied by the base unit to said handset.

8. A method for operating a cordless telephone including a handset having a handset security decode and a base unit including a base unit security code, said method comprising the steps of:

determining when it is desired to update said security codes;

causing a first one of said base unit and said handset to transmit to the other of said handset and said base unit a command indicating said security codes are to be updated and a new value associated with said security codes;

causing the other of said handset and said base unit, upon receipt of said command, to update its security code in accordance with said new value;

upon said updating of said security code of said other of said handset and said base unit, causing said other of said handset and said base unit to send an acknowledgement signal to the first; and

upon receipt by said first of said acknowledgement signal, causing said first to update its security code.

9. A method as in claim 8 wherein said step of determining when a security code update is desired operates in response to stimulus selected from the group consisting of: elapsed time, cordless telephone usage, placement of said handset in said cradle; removal of said handset from said cradle, turning on said handset, turning off said handset, and selection of one or more functions on said handset.

10. A method as in claim 8 wherein said method is interrupted when normal operation of said cordless telephone system takes place during said method, thereby preventing said security codes from being updated.

| | |
|---|---|
| **Patents Act 1977**<br>**Examiner's report to the Comptroller under Section 17 (The Search Report)** | Application number<br>9203592.2 |

| | |
|---|---|
| **Relevant Technical fields**<br>(i) UK Cl (Edition K ) H4L (LECTS)<br>(ii) Int CL (Edition 5 ) H04M 1/66, 66; 1/72 | Search Examiner<br>N W HALL |
| **Databases** (see over)<br>(i) UK Patent Office<br>(ii) | Date of Search<br>22 JUNE 1992 |

Documents considered relevant following a search in respect of claims 1 TO 10

| Category (see over) | Identity of document and relevant passages | Relevant to claim(s) |
|---|---|---|
| X | GB 2217151 A (SONY) page 27 line 28 - page 31 line 11 | 1-4, 7-9 |
| X | GB 2154395 A (SONY) page 6, line 111 - page 7 line 43 | 1, 2, 4, 8, 9 |
| X | EP 0196834 A2 (ATT) page 7 lines 15-29 | 1, 3, 4, 7-9 |
| X | WO 85/02738 A1 (MOTOROLA) page 4 lines 2-4; page 22, line 27 - page 23, line 2 | 1, 3, 4 7-9 |

| Category | Identity of document and relevant passages | Relevant to claim(s) |
|---|---|---|
|  |  |  |

**Categories of documents**

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

**Databases:** The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

Published 1992 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from
Sales Branch, Unit 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.